

REMARKS

Claims 1-76, 78-80, and 82-99 are pending in this application. The non-final Office Action mailed April 28, 2005 rejected claims 1-76, 78-80, and 82-99. Claims 1, 4, 5, 12, 14, 15, 17, 29, 34, 36, 48, 53, 61, 62, 65, 67, 73, 74, 76, 78, 80, 86, 97, and 98 have been amended in the present response to clarify that which is the claimed invention. No new matter has been added by this amendment. Claims 3, 30, and 42 have been cancelled. For the reasons discussed in detail below, Applicants submit that the pending claims are patentable over the references cited by the Examiner. Applicants respectfully request that the Examiner pass this application to issue.

Rejection Under 35 U.S.C. § 112, first paragraph

The Office Action rejected independent Claims 1, 17, 36, 53, 61, 67, 78, and 97 under 35 U.S.C. § 112, first paragraph as failing to comply with the written description requirement. Specifically, the Office Action indicates that the specification does not support the previously added limitation “the inspection being independent of a packet header.”

The specification states that the invention “*examines*, parses and selectively encrypts only the payload (e.g., Media content) portion of the data, leaving the non-payload portion intact . . .” (Emphasis added, spec, pg. 9, lns. 12-14.) The specification also states that the invention “parses the network data and only encrypts the relevant payload part, leaving the non-payload part that may include data such as routing, sizing *and other header data* surrounding the payload part entirely untouched.” (Emphasis added, spec, pg. 15, lns. 15-17.) Accordingly, the non-payload portion may comprise a header that is left untouched.

Nevertheless, applicants have amended independent Claims 1, 17, 36, 53, 61, 67, 78, and 97 to remove the reference to a header since the non-payload portion may already include header data. This is consistent with, and supported by the specification as quoted above, which indicates that only one portion (e.g., the payload (e.g., media content) portion), is examined to determine whether encryption is needed, and the non-payload portion comprises a header.

Consequently, only one portion, namely the payload portion is involved in determining whether to encrypt the payload portion without reference to a header.

The specification also provides support for the amendment regarding recognizing the predefined data type in making the determination whether to encrypt. For example, the specification explains that “if the encryption unit sees a data type that it does recognize (e.g. Multimedia content), then it selectively encrypts on the recognized portion of the data stream.” (Spec., pg. 9, lns. 19-21.) Further, the specification states that the “invention recognizes the streaming protocol and acts on the data rather than requiring specific identification of the file format being transmitted.” (Spec., pg. 18, lns. 6-7.)

For the reasons above, the specification describes the subject matter of the amended claims in such a way as to reasonably convey to one skilled in the art that the inventors, at the time the application was filed, had possession of the claimed invention. Accordingly, the rejection of independent Claims 1, 17, 36, 53, 61, 67, 78, and 97 under 35 U.S.C. § 112, first paragraph should be withdrawn.

Rejection of Claims Under 35 U.S.C. § 103 over Wasilewski, Lampson, and Osmond

The Office Action rejected claims 1-14, 16-21, 23-25, 29-30, 36, 39-40, 42, 48-50, 53-57, 61-63, 65-70, 73-76, 78-80, 84-89, and 94-97 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,420,866 to Wasilewski ("Wasilewski") in view of U.S. Patent No. 5,161,193 to Lampson et al. ("Lampson") and U.S. Patent No. 6,044,468 to Osmond ("Osmond").

For the same reasons discussed above, independent Claims 1, 17, 36, 53, 61, 67, 73, 78, 86, and 97 are amended to remove the header reference and to clarify examining one portion, a payload portion, and recognizing a predefined data type to determine if the one (payload) portion is to be encrypted. For easier readability and consistency with the specification, independent Claims 1, 17, 36, 61, 73, 78, 86, and 97 are also amended to specify at least a payload portion rather than first and second portions. Support is found in numerous parts of the specification, including page 9, lines 8-15 and page 15, lines 14-17. Correspondingly, Claims 3, 30, and 42 are cancelled.

The cited prior art references do not disclose or suggest all of the limitations of the amended claims. For example, applicants respectfully disagree that Lampson discloses or suggests determining if a payload portion is to be encrypted by examining the payload portion, especially to recognize a predefined data type as required by the amended claims. In describing the processing of transmitted data packets received from a ring memory controller (RMC) on its way to a media access control (MAC) interface, Lampson states that “[t]he loopback/transmit control state machine must determine from header information in the transmitted packet whether encryption is required . . .” (Lampson, col. 10, lns. 15-19.) Applicants have amended the rejected independent Claims 1, 17, 36, 61, 73, 78, 86, and 97 to indicate a payload portion and a non-payload portion. It is well known in the art that a payload comprises the data of interest in a set of data being communicated. (See also, spec., pg. 8, lns. 7-8.) Lampson states that “packets have their *data portions* encrypted if called for . . .” (emphasis added, Lampson, abstract.) Lampson also provides examples of data packets in figures 9a-10 and 14a-14c that show data portions comprising the payload. In particular, each example packet contains a protected field comprising a session protocol data unit (SPDU) that is well known in the “most widely accepted model [] known as the International Standards Organization (ISO) Open Systems Interconnection (OSI) reference model.” (Lampson, col. 1, lns. 47-50.) Lampson distinguishes this payload from all of the header information provided in the packets of figures 9a-10 and 14a-14c. For example, Lampson explains that a transmit data path will “perform the appropriate transformation and routing of data that follow the header information.” (Lampson, col. 10, lns. 20-22.) The header information is clearly non-payload information. As applicants have argued in response to previous office actions, Lampson discloses detail information how the headers are evaluated to determine whether the payload data should be encrypted. (See Lampson, col. 13, ln. 34 through col. 14, ln. 68.) Thus, Lampson does not disclose or suggest determining if the payload portion is to be encrypted by examining the payload portion to recognize a predefined data type, as required by amended independent Claims 1, 17, and 36. Accordingly, the rejection under 35 U.S.C. § 103(a) of at least independent Claims 1, 17, and 36 should be withdrawn.

Similarly, Osmand does not disclose or suggest determining if the payload portion is to be encrypted by examining the payload portion to recognize a predefined data type. Osmand discloses an encryption service inspecting an actual object ID and request ID to determine whether encryption is needed. (Osmand, col. 8, lns. 33-35.) The encryption service must determine whether an object ID value corresponds to a network management instruction to a agent that should be encrypted to prevent inadvertent or malicious change in critical data that could cause a disruption in service of a communication network. (See Osmand, col. 8, lns. 36-58.) Inspecting a network management instruction does not disclose or suggest recognizing a predefined data type.

In addition, there is no suggestion or motivation to select and combine Osmand with Lampson. Osmand discloses an application-level protocol, including simple network management protocol (SNMP), regarding command messages for remotely managing network elements “and not the particular manner in which the messages are transmitted.” (Osmand, col. 1, lns. 15-26 and col. 6, ln. 3.) As is well known in the art, the application level is the highest layer (layer 7) of the ISO/OSI model. In contrast, Lampson is directed to sublayers of the data link layer. (Lampson, col. 1, ln. 65 through col. 2, ln. 26, and col. 6, lns. 44-49.) As is also well known in the art, the data link layer is the second lowest layer (layer 2) of the ISO/OSI model and is directed to how packets are transmitted. Osmand and Lampson do not disclose, suggest, or provide any motivation to modify or combine each other’s teachings for use in either of the vastly different layers to which Osmand and Lampson are directed.

There is also no suggestion or motivation to combine Osmand or Lampson with Wasilewski. Wasilewski is directed to a transport layer (layer 4) method for transmitting conditional access information to decoders that will receive encrypted data such as subscription television broadcasts. (See Wasilewski, col. 1, lns. 35-38, col. 1, ln. 61 through col. 2, ln. 3, and col. 4, ln. 51 through col. 5, ln. 62.) Further, Wasilewski does not disclose or suggest that a determination is needed on whether to encrypt a payload. Wasilewski specifies that conditional access information is encryption related information. (Wasilewski, col. 4, lns. 9-10.) For the conditional access information to be of any use, the payload data, such as a subscription television broadcast, must be encrypted. Thus, there is no motivation to modify or combine Wasilewski with

Lampson or Osmand which both require a determination on whether to encrypt certain payload data or not.

For the reasons above, the rejection under 35 U.S.C. § 103(a) of independent Claims 1, 17, 36, 53, 61, 67, 73, 78, 86, and 97 over Wasilewski in view of Lampson and Osmand should be withdrawn. Dependent claims are patentable for at least the same reasons as the independent claims from which the dependent claims depend. Accordingly, the rejection under 35 U.S.C. § 103(a) of dependent Claims 2-14, 16, 18-21, 23-25, 29, 30, 39, 40, 42, 48-50, 54-57, 62, 63, 65, 66, 68-70, 74-76, 79, 80, 84, 85, 87-89, and 94-96 over Wasilewski in view of Lampson and Osmand should also be withdrawn.

Rejection Under 35 U.S.C. § 103 over Wasilewski, Lampson, Osmond and Graunke

The Office Action rejected dependent Claims 15, 26-28, 31-35, 37, 38, 43-47, 52, 64, 71, 72, 82, 83, 90-93, and 99 under 35 U.S.C. § 103(a) as being unpatentable over Wasilewski, Lampson, and Osmond as applied to Claims 1, 17, 36, 45, 61, 70, 81, 88, and 97, and further in view of U.S. Patent No. 5,991,399 to Graunke et al (“Graunke”). The office action does not indicate that Graunke discloses or suggests the limitations that are missing from Lampson and Osmond as discussed above. Graunke is directed to distribution of conditional use information (e.g. a private key) for access to encrypted payload data. Thus, Graunke would have no use for the determining whether to encrypt payload data as disclosed by Lampson and Osmond. Similar to Wasilewski, there is no suggestion or motivation to combine Graunke with Lampson or Osmond. Accordingly, dependent Claims 15, 26-28, 31-35, 37, 38, 43-47, 52, 64, 71, 72, 82, 83, 90-93, and 99 are patentable for at least the same reasons as the independent claims from which these dependent claims depend, and the rejection under 35 U.S.C. § 103(a) should be withdrawn.

Rejection Under 35 U.S.C. § 103 over Wasilewski, Lampson, Osmond, Graunke and Dorfman

The Office Action rejected dependent Claims 22, 41, 51, 58, and 59 under 35 U.S.C. § 103(a) as being unpatentable over Wasilewski, Lampson, and Osmond as applied to Claims 20, 39, and 57, and further in view of Graunke and U.S. Patent No. 6,449,651 to Dorfman et al

("Dorfman"). The office action does not indicate that Dorfman discloses or suggests the limitations that are missing from Lampson and Osmond as discussed above. Dorfman is directed to providing temporary access to a computer using an encryption algorithm and a key. Thus, Dorfman would have no use for determining whether to encrypt payload data as disclosed by Lampson and Osmond. Similar to Wasilewski, there is no suggestion or motivation to combine Dorfman with Lampson or Osmond. Accordingly, dependent Claims 22, 41, 51, 58, and 59 are patentable for at least the same reasons as the independent claims from which these dependent claims depend, and the rejection under 35 U.S.C. § 103(a) should be withdrawn.

Rejection Under 35 U.S.C. § 103 over Wasilewski, Lampson, Osmond, and Fawcett

The Office Action rejected dependent Claim 98 under 35 U.S.C. § 103(a) as being unpatentable over Wasilewski, Lampson, and Osmond as applied to Claim 97, and further in view of U.S. Patent No. 5,678,002 to Fawcett et al ("Fawcett"). Fawcett is directed to exchanging diagnostic and solution data between a client and server to provide automated customer support. However, the office action does not indicate that Fawcett discloses or suggests the limitations that are missing from Lampson and Osmond as discussed above. Accordingly, dependent Claim 98 is patentable for at least the same reasons as the independent claims from which this dependent claim depends, and the rejection under 35 U.S.C. § 103(a) should be withdrawn.

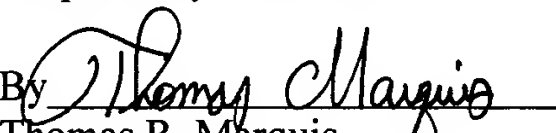
CONCLUSION

By the foregoing explanations, Applicants believe that this response has responded fully to all of the concerns expressed in the Office Action, and believes that it has placed each of the pending claims in condition for immediate allowance. Accordingly, the Examiner is respectfully requested to pass this application to issue. Should any further aspects of the application remain unresolved, the Examiner is invited to telephone applicant's attorney at the number listed below.

Dated: July 28, 2005

Customer No.: 07278

Respectfully submitted,

By 
Thomas R. Marquis
Registration No.: 46,900
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(206) 262-8900
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant